REMARKS

This amendment is responsive to the Office Action dated May 8, 2006. In the amendment, claims 1, 13, 35 and 46 have been amended. Claims 25-34 were previously withdrawn from consideration and claims 1-24 and 35-46 remain pending in the application. Reconsideration of the pending claims in light of these amendments and the following remarks is respectfully requested. These amendments add no new matter.

The title has been objected to for various reasons, which are believed to be addressed in the new title submitted herewith. Specifically, the title has been amended to read "Encryption of Information Input to Portable Card Terminal using Encryption Key Information associated to Portable Card Terminal Identifier." The Examiner is invited to make additional suggestions regarding the title if it remains objectionable.

Claim 1 has been objected to for containing the phrase "an encryption key information". This phrase has been changed to "encryption key information". Applicant submits that the amendment to the claim obviates this objection to the claim.

Claims 1-24 and 35-46 have been rejected under 35 U.S.C. § 112, ¶2, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Specifically, the Examiner objected to the phrase "pre-stored". Applicant has amended the claims to use the phrase "stored", which is believed to address the Examiner's objection in this regard. Applicant submits that the claims are recited with the requisite clarity and distinctiveness, and requests reconsideration and withdrawal of the rejection of the claims under 35 U.S.C. § 112, ¶2.

Claims 1-9, 13-21 and 35-42 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 5,880,769 to Nemirofsky ("Nemirofsky") in view of B. Schneier, "Applied Cryptography," John Wiley & Sons, 1996, pp. 170-178 ("Schneier"). This rejection is traversed.

Claim 1 has been amended and now recites: *[a]n authentication system, said authentication system comprising:*

a portable card terminal, including:

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on encryption key information, and

first communication means for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device, provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification information and the second identification information therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and

comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said

authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.

These claimed features are not disclosed or suggested by Nemirofsky or Schneier, alone or in any combination.

Nemirofsky discloses a smart card that stores account information for remote financial services. A connection with a financial institution is initiated through the smart card, and data is exchanged to carry out a fully automated transaction. A user may also be required to enter a PIN code that is associated with the smart card, for enhanced security. However, there is no mention whatsoever of encrypting the PIN code.

The Schneier reference discloses that it is known to generate encryption keys, and that these keys are used to encrypt sensitive information that is sent between parties or devices. Based upon this disclosure, the Examiner apparently concludes that it would be obvious to encrypt the smart card PIN code of Nemirofsky based upon the teachings of Schneier.

Applicant has amended claim 1 to clarify the authentication features involving the first identification information (e.g., the portable card terminal ID), the generation of the encryption key, and the corresponding encryption of the second identification information input to the portable card terminal. Specifically, (1) the "first identification information" (card ID) is sent from the portable card terminal to the authentication device, (2) the authentication device then generates the encryption key and sends it back to the portable terminal device, and (3) the portable terminal device then uses the encryption key to encrypt the second identification information and send it to the authentication device, which then performs authentication.

Even assuming that Nemirofsky and Schneier disclose what is described above, at most a combination of those references would suggest that the smart card PIN code of Nemirofsky *could* be encrypted, generally. This, however, would not disclose the particular authentication

features claimed by Applicant. With Applicant's claimed invention the card ID is sent to the authentication device, then the authentication device generates the encryption key information and forwards the so-generated encryption key information to the portable card terminal. Only then does the portable card terminal encrypt the second identification information that has been input, using the so-generated encryption key information. There is no disclosure or suggestion of these particular features of Applicant's claimed invention, even in the combination proposed by the Examiner.

The Examiner cites Nemirofsky's disclosure of a smart card serial number as a possible portable card identifier as claimed. However, even assuming this to be correct, there still would be no disclosure or suggestion of the authentication features claimed by Applicant. Concluding as such would require significant conjecture. That is, one would have to conclude that the smart card serial number is sent out, that an encryption key is then generated and then returned to the smart card, with the smart card then using that encryption key to encrypt the PIN number. Given that Nemirofsky does not even generally disclose encrypting the PIN number, it cannot be fairly concluded that the general encryption teaching of Schneier would disclose, suggest, or in any way motivate the artisan to provide such features.

The Examiner also states that the encryption key itself could be the "first identification information." However, it is not seen how this view comports with the claimed invention. That is, if the encryption key itself is "first identification information," there would still be no disclosure of sending that information from the portable card terminal to the authentication device, generating encryption key information in response to receiving that information, sending the so-generated encryption key information to the portable card terminal, and then encrypting the second information using the so-generated encryption key information. Moreover, the encryption key would not be a portable card terminal *identifier*.

Accordingly, Applicant submits that a *prima facie* case of obviousness has not been established for independent claim 1. The remaining independent claims are also neither disclosed nor suggested by the combination of Nemirofsky and Schneier, for reasons similar to those provided regarding claim 1, as they have been similarly amended. The cited dependent claims are also neither disclosed nor suggested by the relied upon references, for their respective

incorporation of the features recited in the independent claims, as well as their separately recited, patentably distinct features.

Claims 10-12, 22-24 and 43-46 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemirofsky in view of Schneier, and further in view of Lillibridge. This rejection is traversed.

Lillibridge does not remedy the deficiencies of Nemirofsky and Schneier as described above. Lillibridge appears to disclose a string that may be randomly modified to form a riddle, and offers no disclosure or suggestion of the features recited in Applicant's independent claims. That is, Lillibridge also fails to disclose or suggest, *inter alia*, sending the first identification information from the portable card terminal to the authentication device, having the authentication device then generate the encryption key and send it back to the portable card terminal, and having the portable card terminal use the encryption key to encrypt the second identification information and send it to the authentication device, which then performs authentication.

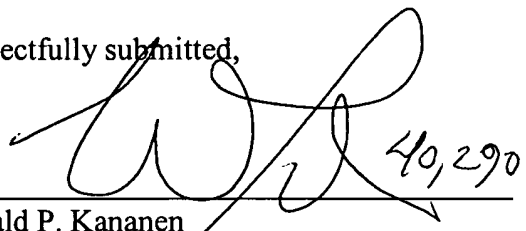
The claims are thus still neither disclosed nor suggested by the three reference combination of Nemirofsky, Schneier, and Lillibridge. The dependent claims are also neither disclosed nor suggested by the relied upon references, for their respective incorporation of the features recited in the independent claims, as well as their separately recited, patentably distinct features.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of the cited claims as being unpatentable over Nemirofsky in view of Schneier, and further in view of Lillibridge.

For the foregoing reasons, reconsideration and allowance of the claims which remain in this application are solicited. If any further issues remain, the Examiner is invited to telephone Christopher M. Tobin at (202) 955-8779 to resolve them.

Dated: August 8, 2006

Respectfully submitted,



By _____
Ronald P. Kananen
Registration No.: 24,104
Christopher M. Tobin
Registration No.: 40,290
Attorney for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building, 1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750; Fax: (202) 955-3751
Customer No. 23353